JOURNAL OF COMBINATORIAL THEORY, Series A 25, 84–89 (1978)

Note

Pairwise "Orthogonal Generalized Room Squares" and Equidistant Permutation Arrays

S. A. VANSTONE

Department of Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

Communicated by the Managing Editors

Received February 16, 1977

A generalized Room square $S(r, \lambda; v)$ is an $r \times r$ array such that every cell in the array contains a subset of a v-set V. This subset could of course be the empty set. The array has the property that every element of V is contained precisely once in every row and column and that any two distinct elements of V are contained in precisely λ common cells. In this paper we define pairwise orthogonal generalized Room squares and give a construction for these using finite projective geometries. This is another generalization of the concept of pairwise orthogonal latin squares. We use these orthogonal arrays to construct permutations having a constant Hamming distance.

1. INTRODUCTION

A *generalized Room square* (G.R.S.) $S(r, \lambda: v)$ is an $r \times r$ array such that (i) every cell in the array contains a subset (possibly empty) of a v-set V, (ii) every element of V is contained precisely once in every row and column and (iii) any two distinct elements of V are contained in exactly λ common cells. Let S_l and S_k be an $S(r, \lambda; v)$ defined on V and an $S(r, \lambda; v_k)$ defined on V_k, respectively, where $|V_t| = v_t$, $t = l, k$. Let B_{ij} and C_{ij} be the subsets contained in the ijth cell of S_l and S_k, respectively. We say that S_l and S_k are *orthogonal* of index λ^* if for every pair (a, b), $a \in V_l$, $b \in V_k$

$$|\{(i, j): a \in B_{ij}, b \in C_{ij}\}| = \lambda^*.$$

A set $\{S_i(r, \lambda; v_i): 1 \leqslant i \leqslant t\}$ is called *a set of pairwise orthogonal generalized Room squares* (P.O.G.R.S.) of index λ^* if every pair of distinct squares in the set is orthogonal of index λ^*.

It is clear that a Latin square of order n is an $S(n, o; n)$ and that a set of pairwise orthogonal Latin squares of order n is a set of pairwise orthogonal generalized Room squares of index 1.

0097-3165/78/0251–0084$02.00/0

An *equidistant permutation array* (E.P.A.) is a $v \times r$ array $A(r, \lambda: v)$ such that every row is a permutation of a set of r symbols and any two distinct rows have precisely λ common column entries. Another way of stating the last property is to say that the Hamming distance between any two distinct rows is $r - \lambda$. It has been shown [4] that an $A(r, \lambda: v)$ is equivalent to an $S(r, \lambda: v)$. In the next section we construct an infinite family of pairwise orthogonal generalized Room squares and use them to construct equidistant permutation arrays. We require several more definitions.

An (r, λ)-*design* D is a collection of subsets (called blocks) taken from a finite set V of elements (called varieties) such that every variety of V is contained in precisely r blocks and every pair of distinct varieties is contained in exactly λ of the blocks. If $|V| = v$ we denote such an (r, λ)-design by $D(r, \lambda; v)$.

A $D(r, \lambda; v)$ is said to be *resolvable* if the blocks of D can be partitioned into classes $R_1, R_2, \ldots, R_r$ (called resolution classes) such that every variety of D is contained in precisely one of the blocks of each class. A resolvable (r, λ)-design is called an *orthogonal* (r, λ)-*design* if the blocks of D can be partitioned in a second way into resolution classes $R_1', R_2', \ldots, R_r'$ such that for any i, j, $1 \leqslant i, j \leqslant r$.

$$|R_i \cap R_j| \leqslant 1.$$

(We note that the blocks of a design are considered to be labeled blocks so that repeated blocks are considered distinct.) We denote an orthogonal (r, λ)-design on v varieties by $OD(r, \lambda: v)$. The following theorem is proved in [4].

THEOREM 1.1. *The existence of any one of the following implies the existence of the other two.*

(1) $S(r, \lambda: v)$;

(2) $A(r, \lambda: v)$;

(3) $OD(r, \lambda: v)$.

2. PRELIMINARY CONSTRUCTIONS

The following result is self evident.

THEOREM 2.1. *Let* $T = \{S_i(r, \lambda: v_i): 1 \leqslant i \leqslant t\}$ *be a set of pairwise orthogonal generalized Room squares of index* λ. *Then* T *exists iff there exists an* $S(r, \lambda; \sum_{i=1}^{t} v_i)$.

The next theorem is a straightforward generalization of a construction due to Woodall [8].

THEOREM 2.2. *Let* $T = \{S_i(r, \lambda; v_i): 1 \leqslant i \leqslant t\}$ *be a set of* t *P.O.G.R.S. of index* λ^* *where* $\lambda^* > \lambda$ *and* E *be an* $A(r', \lambda'; v)$ *where* $v \geqslant t$ *such that* $(\lambda^* - \lambda) \mid (r' - \lambda')$. *Then there exists an* $A(xr + r', x\lambda + r'; \sum_{i=1}^{t} v_i)$ *where* $x = r' - \lambda'/\lambda^* - \lambda$.

Proof. By Theorem 1.1 each $S(r, \lambda; v_i)$ $(1 \leqslant i \leqslant t)$ is equivalent to an $A(r, \lambda; v_i)$. Let $A_j(r, \lambda; v_i)$ be an $A(r, \lambda; v_i)$ defined on the symbols $1_j, 2_j, \ldots, r_j$ for $1 \leqslant j \leqslant x$. Let L_i $(1 \leqslant i \leqslant v)$ be a $v_i \times r'$ array where each row is a copy of row i of $A(r', \lambda'; v)$. Consider the following $(\sum_{i=1}^{t} v_i) \times (xr + r')$ array.

$A_1(r, \lambda; v_1)$	$\cdots$	$A_j(r, \lambda; v_1)$	$\cdots$	$A_x(r, \lambda; v_1)$	L_1
$A_1(r, \lambda; v_2)$	$\cdots$	$A_j(r, \lambda; v_2)$	$\cdots$	$A_x(r, \lambda; v_2)$	L_2
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$\vdots$		$\vdots$		$\vdots$	$\vdots$
$A_1(r, \lambda; v_t)$	$\cdots$	$A_j(r, \lambda; v_t)$	$\cdots$	$A_x(r, \lambda; v_t)$	L_t

Consider two distinct rows of the array. If the two rows both contain rows from L_i then they have $x\lambda + r'$ columns in common. Suppose one of the two rows contains a row of L_i and one a row from L_j $(i \neq j)$. The two rows have $x\lambda^* + \lambda'$ columns in common since the set of P.O.G.R.S.'s are orthogonal of index λ^*.

Since

$$x = r' - \lambda'/\lambda^* - \lambda,$$

$$x\lambda + r' = x\lambda^* + \lambda'.$$

Hence any two distinct rows of the array have precisely the same number of columns in common.

It is clear that every row of the array is a permutation of a set of $xr + r'$ symbols. This completes the proof.

A class of E.P.A.'s which are very useful is given in the next theorem.

THEOREM 2.3. *There exists an* $A(n, n - 3; n - 1)$.

Proof. Consider a set V of $n - 1$ varieties. Form an (r, λ)-design D on the set V consisting of all $(n - 2)$-subsets of the $(n - 1)$-set V and $2(n - 1)$ blocks of size one such that every element of V is contained in two blocks of size one. It is easy to check that D is an $OD(n, n - 3; n - 1)$. By Theorem 1.1, D implies the existence of an $A(n, n - 3; n - 1)$. ∎

3 Finite Geometries and E.P.A.s

If each block of an (r, λ)-design D has cardinality k then D is called a balanced incomplete block design (BIBD). If D has v varieties and b blocks the parameters of D are denoted (v, b, r, k, λ).

For the definition of a finite affine geometry of order q and dimension n the reader is referred to [1]. It is known that for $n \geqslant 3$, q must be a power of a prime. A finite affine geometry of order q and dimension n, denoted $AG(n, q)$, can be used to form a BIBD if we use the points of the geometry as varieties and the hyperplanes as blocks. Such a design has parameters

$$\left(q^n, \frac{q(q^n - 1)}{q - 1}, \frac{q^n - 1}{q - 1}, q^{n-1}, \frac{q^{n-1} - 1}{q - 1}\right).$$

Since the hyperplanes of an $AG(n, q)$ can be partitioned into parallel classes, the corresponding BIBD is a resolvable block design. Any two blocks from different resolution classes have precisely q^{n-2} varieties in common. We shall give a construction for a set of P.O.G.R.S. of index λ^* using such configurations.

Before stating and proving the next result we require a definition. If D is an (r, λ)-design defined on the variety set V and $V_1 \subseteq V$, then the *restriction* of D to V_1, denoted by $D(V_1)$, is the (r, λ)-design defined on V_1 such that if B is a block of D then $B \cap V_1$ is a block of $D(V_1)$.

Theorem 3.1. *If q is a prime power and n is a positive integer greater than 1 then there exists a set $(T = \{S_i(r, \lambda; v_i): r = v_i = q^{n-1}, \lambda = q(q^{n-2} - 1)/q - 1, 1 \leqslant i \leqslant q^{n-1} - 1\}$ and $v_i = q^{n-1}\})$ of pairwise orthogonal generalized Room squares of index $q^{n-1} - 1/q - 1$.*

Proof. Consider an affine geometry $AG(n, q)$ and the resolvable BIBD whose blocks are the hyperplanes of the geometry. The parameters of the block design D are

$$\left(q^n, \frac{q(q^n - 1)}{q - 1}, \frac{q^n - 1}{q - 1}, q^{n-1}, \frac{q^{n-1} - 1}{q - 1}\right).$$

Let $P_0, P_1, P_2, \ldots, P_{r-1}$ where $r = q^n - 1/q - 1$ be the resolution classes (parallel classes) of D and B_{ij} $(1 \leqslant j \leqslant q)$ be the blocks of P_i.

The varieties of B_{01} are the points in a hyperplane. Let B_{01} also represent this hyperplane and consider the $n - 2$ dimensional spaces contained in B_{01}. We denote these by $H_1, H_2, \ldots, H_t$ where $t = q(q^{n-1} - 1)/q - 1$. Define

$$Q_{H_i} = \{B \backslash H_i : B \text{ is a block of } D,\ H_i \subseteq B,\ B \neq B_{01}\}, \qquad 1 \leqslant i \leqslant t.$$

Let D' be the design obtained from D by deleting the varieties of B_{01}. Let $P_i' = \{B_{ij} \backslash B_{01} : 1 \leqslant j \leqslant q\}$, $0 \leqslant i \leqslant r - 1 = t$. Now $P_0', P_1', \ldots, P_r'$ is a resolution of D' and $P_0 \backslash B_{01}, Q_{H_1}, Q_{H_2}, \ldots, Q_{H_t}$ is another resolution of D' such that $|P_i' \cap Q_{H_j}| \leqslant 1$ for $1 \leqslant i, j \leqslant r - 1 = t$.

Consider the restriction $P(B_{0i})$, $2 \leqslant i \leqslant q$, and define $P_k' \cap B_{0i} = \{B_{ij} \cap B_{0i} : 1 \leqslant j \leqslant q\}$, $1 \leqslant k \leqslant r$, and $Q_{H_k} \cap B_{0i} = \{(B \backslash H_i) \cap B_{0i} : B$ is a block of D and $H_i \subseteq B\}$. If $P^i = \{P_k' \cap B_{0i} : 1 \leqslant k \leqslant r\}$ and $Q^i = \{Q_{H_k} \cap B_{0i} : 1 \leqslant k \leqslant r\}$ then P^i and Q^i are two resolutions of $D(B_{0i})$ having the property that

$$|(Q_{H_k} \cap B_{0i}) \cap (P_l' \cap B_{0i})| \leqslant 1, \qquad 1 \leqslant k, \quad l \leqslant r.$$

Hence $D(B_{0i})$ is an $OD(r, \lambda; q^{n-1})$ where $\lambda = q(q^{n-2} - 1)/q - 1$. If B is a block of $D(B_{0i})$ and $B \in P_j' \cap B_{0i}$ and $B \in Q_{H_l} \cap B_{0i}$ then B will occur in the (j, l) cell of an array $S_i(r, \lambda; q^{n-1})$. This is the construction of Theorem 1.1. Now, if $a \in B_{0i}$ and $b \in B_{0j}$ $(i \neq j)$, a and b are contained in $\lambda^* = q^{n-1} - 1/q - 1$ blocks of D. This implies that in $S_i(r, \lambda; q^{n-1})$ there are precisely λ^* cells containing a and the corresponding cells in $S_j(r, \lambda; q^{n-1})$ contain b. Hence $S_i(r, \lambda; q^{n-1})$ and $S_j(r, \lambda; q^{n-1})$ are orthogonal of index λ^*. Therefore

$$T = \{S_i(r, \lambda; q^{n-1}) : 2 \leqslant i \leqslant q\}$$

is a set of $q - 1$ pairwise orthogonal generalized Room squares of index λ^*.

We now apply the results of Section 2.

THEOREM 3.2. *For q a prime power and n a positive integer there exists an*

$$A\left(\frac{3q(q^{n-1} - 1)}{q - 1} + q, \frac{3q(q^{n-2} - 1)}{q - 1} + q; (q - 1)\, q^{n-1}\right).$$

Proof. By Theorem 2.3 there exists an $A(q, q - 3; q - 1)$. Applying Theorem 2.2 to this and the set of pairwise orthogonal generalized Room squares of Theorem 3.1, we obtained the stated result.

In the special case of $n = 2$ and q a prime power we obtain the Woodall result [8] that there exists an $A(4q, q; q(q - 1))$.

4. CONCLUSION

It should be noted that the G.R.S.'s constructed in Theorem 3.1 all have nonempty subsets of constant cardinality. Such arrays we call *uniform*. Room squares [6] provide another class of uniform G.R.S.'s.

When constructing $A(r, \lambda; v)$ s it is desirable to have v as large as possible. It has been shown by Deza [2] that

$$v \leqslant \max\{r^2 - r + 1, \lambda + 2\}.$$

In certain cases this bound can be realized. It has been shown [3] that in an $A(r, 1; v)$, $v \leqslant r(r-3)$ for $r \geqslant 4$. This has been imporoved [7] to $v \leqslant r(r-4)$, but it is not known whether this is best possible.

It has been shown [5] that there exists an $A(r, 1; 2r-4)$ for all $r \geqslant 6$. No one has as yet constructed an $A(r, 1; v)$ where $v \geqslant 2r$. For $\lambda > 1$, this does occur as shown by Theorem 3.2.

REFERENCES

1. I. BLAKE AND R. C. MULLIN, "The Mathematical Theory of Coding," Academic Press, New York.
2. M. DEZA, Metrices dont deux lignes quelconques coincident dans un nombre donne de positions communes, *J. Combinatorial Theory Ser. A*, to appear.
3. M. DEZA, R. C. MULLIN, AND S. A. VANSTONE, Orthogonal systems, *Aequationes Math.*, to appear.
4. M. DEZA, R. C. MULLIN, AND S. A. VANSTONE, Room squares and equidistant permutation arrays, *Ars Combinatoria* **2** (1976), 235–244.
5. K. HEINRICH AND J. VAN REES, Equidistant permutation arrays of index 1, *Utilitas Math.*, submitted.
6. R. C. MULLIN AND W. D. WALLIS, The existence of Room squares, *Aequationes Math.* **13** (1975), 1–7.
7. R. C. MULLIN AND E. NEMETH, "An Improved Bound for Equidistant Permutation Arrays of Index 1, preprint.
8. D. R. WOODALL, unpublished manuscript.